WEST VIRGINIA DEPARTMENT OF TRANSPORTATION

ADMINISTRATIVE PROCEDURES

SUBJECT: GENERAL

CHAPTER TITLE: PROPER USE OF INFORMATION TECHNOLOGY

Effective: 12/15/2007

THE DEPARTMENT'S COMPUTERS AND OTHER TECHNOLOGICAL RESOURCES AND EQUIPMENT, AS WELL AS THE NETWORK, DOT'S EMAIL SYSTEM AND INTERNET ACCESS, ARE FOR OFFICIAL USE. THEREFORE, ANY INFORMATION PLACED, CREATED OR TRANSMITTED IN OR THROUGH ANY OF THESE RESOURCES BELONGS TO THE DOT, AND THAT INFORMATION, AS WELL AS ANY INFORMATION ACCESSED FROM THESE RESOURCES, MAY BE MONITORED, SEARCHED, ACCESSED, USED, DISCLOSED, AND/OR PRESERVED BY THE DOT. THE ASSIGNMENT OR USE OF A USER ID AND/OR PASSWORD IS NOT AN INDICATOR OF PRIVACY.

THE USE OF ANY DOT COMPUTER OR TECHNOLOGICAL EQUIPMENT CONSTITUTES CONSENT TO THESE POLICIES. THERE IS NO RIGHT OF PRIVACY IN THESE SYSTEMS AND EQUIPMENT, THEIR CONTENT, OR USE.

SUBJECT: GENERAL

CHAPTER TITLE: PROPER USE OF INFORMATION TECHNOLOGY

Effective: 12/01/2008

I. INTRODUCTION

II. POLICIES

A. AUTHORIZED USE
B. PROHIBITED USES
C. PRIVACY, AGENCY ACCESS, AND MONITORING OF EMPLOYEE COMMUNICATIONS AND AGENCY RESOURCES

1. PRIVACY
2. WHO MAY REQUEST
3. CONTENT OF REQUESTS
4. REQUEST PROCESS

D. BROADCASTING E-MAIL MESSAGES
E. INQUIRIES AND POTENTIAL INFRACTIONS

III. PENALTIES FOR VIOLATING POLICIES

IV. APPENDICES

A. PROPER USE OF INFORMATION TECHNOLOGY POLICY ACKNOWLEDGEMENT STATEMENT

V. WVOT-PR1001 FORM REQUESTING A TECHNICAL INVESTIGATION OF AN EMPLOYEE

SUBJECT: GENERAL

CHAPTER TITLE: PROPER USE OF INFORMATION TECHNOLOGY

I. INTRODUCTION

Effective: 12/15/2007

Modern technological advances have provided many benefits to the Department of Transportation (DOT). They allow the DOT to maximize the efficiency and productivity of its workforce by processing information more quickly, with greater accuracy, and with less effort than ever before. These advances include but are not limited to computers; printers; software; video imaging or duplication equipment; facsimile (FAX) machines; cameras; telephones (landline, cellular and camera); handheld devices (two-way mobile radios, personal digital assistants, etc.); electronic mail (e-mail); the DOT network; the DOT intranet; and the internet (world wide web).

The Department of Administration, Office of Technology is charged with the development and control of technological resources. Within the DOT, Information Services Division is charged with fulfilling these responsibilities and with formulating relevant policies.

II. POLICIES

Effective: 12/15/2007

A. AUTHORIZED USE

Subject to supervisory discretion, employees are authorized to use information technology resources that are necessary or appropriate to perform their job functions.

B. **PROHIBITED USES**

Certain use of state-owned technological equipment is prohibited, including but not limited to the following activities:

1. Using for, or in support of, unlawful, improper, or prohibited activities as defined by federal, state, and local laws or regulations or applicable state agency policy.
2. Violating applicable civil or criminal laws, regulations, policies, or agreements governing software licensing, copyright, and other information or communications technology issues.
3. Accessing, storing, or transmitting potentially threatening, offensive, or harassing information (messages, images, or other media), including but not limited to material that could be construed as insulting, abusive, threatening, offensive, obscene, pornographic, profane, sexually oriented or sexually explicit, defamatory, harassing, or discriminatory, or otherwise inappropriate or illegal.
4. Distributing State, employee, or other confidential data and information without proper authorization or cause.
5. Attempting to gain unauthorized access to any system, resource, or equipment.
6. Using technological resources without authorization or for an unauthorized or improper purpose.
7. Using someone else's password or sharing a password with anyone else without authorization.
8. Attempting to undermine network security, to impair network functionality, or to bypass restrictions set by system administrators.
9. Releasing any type of virus or harmful computer program.
10. Attempting to use system privileges after transfer or termination.

11. Distributing "junk" mail including but not limited to: pyramid schemes, chain letters, jokes, advertisements, unauthorized solicitations, and/or non-business related hyperlinks, pictures, or media files.
12. Encrypting any e-mail communication without authorization.
13. Broadcasting e-mail messages without authorization, as described in §II.D. of this Policy.
14. Using agency e-mail to create non-business online shopping accounts, subscriptions, newsletters, newsgroups, and the like, or to send/receive non-business e-mail or updates.
15. Conducting private or personal activities for personal gain or profit.
16. Conducting not-for-profit activities, including non-government-related fund-raising or public relations activities such as solicitations for religious and political causes, campaign activities or political activities of a partisan nature.
17. Using agency resources, including but not limited to email, computers, and the agency internet connection for personal and non-business reasons and in a manner or with such frequency that would tend to interfere with the performance of official duties or create a reasonable perception of such interference.

C. **PRIVACY, AGENCY ACCESS, AND MONITORING OF EMPLOYEE COMMUNICATIONS AND AGENCY RESOURCES**

1. **PRIVACY**

The Department's computers and other technological resources and equipment, as well as the network, DOT's email system and internet access, are for official use. Therefore, any information placed, created or transmitted in or through any of these resources belongs to the DOT, and that information, as well as any information accessed from these resources, may be

monitored, searched, accessed, used, disclosed, and/or preserved by the DOT. The assignment or use of a User ID and/or password is not an indicator of privacy.

The use of any DOT computer or other technological equipment constitutes consent to these policies. There is no right of privacy in these systems and equipment, their content, or use.

2. **WHO MAY REQUEST**

DOT Agency Heads/Commissioners, Division Directors and District Engineers/Managers may request that employee communications and the resources used therefore be monitored, searched or accessed. (See Request Form)

3. **CONTENT OF REQUESTS**

Requests should be in writing and signed by the requesting party. Requests should include, when reasonably available and applicable, identification information (author, recipient, date, subject, file name, description of content, etc.) and a brief description of the reason(s) access or monitoring is requested.
(See Request Form)

4. **REQUEST PROCESS**

a. Division of Highways:
   (1) General Rule: Except as denoted below, written requests must be directed to the Director of Transportation Human Resources Division. Upon receipt, the Human Resources Director, or his or her designee, will confer with the Director of Legal Division, or his or her designee. If the designated parties agree to grant the request, the Director of Human Resources will forward the approved request to the

Director of the Information Technology Division, his or her designee, or other appropriate party for execution. If the designated parties agree that the request should be denied, authorization will be refused. If the designated parties disagree regarding treatment of the request, the Commissioner of Highways, or his or her designee, shall determine the outcome of the request.

(2) Exceptions:

(a) Legal: If litigation in any form is pending, anticipated, or probable, in the sole judgment of the Director of the Legal Division, said Director may authorize and instruct the Director of Information Services, his or her designee, or other appropriate party to monitor, search, access, use, disclose, and/or preserve any and all forms of electronic communication or information of potentially involved or interested parties.

(b) Immediate Access: If immediate access is desired, the requesting party should contact the Director of Transportation Human Resources Division by telephone, who shall determine the outcome of the request.

b. Other Transportation Agencies:

(1) General Rule: Except as denoted below, all written requests must be directed to the Director of Transportation Human Resources Division. Upon receipt, the Human Resources Director, or his or her designee, will confer with the Commissioner, Executive Director, or Director of the relevant entity or his or her designee. If the designated parties agree to grant the request, the

Director of Human Resources will forward the approved request to the Director of Information Services, his or her designee, or other appropriate party for execution. If the designated parties agree that the request should be denied, authorization will be refused. If the designated parties disagree regarding treatment of the request, the Secretary of Transportation, or his or her designee, shall determine the outcome of the request.

(2) Immediate Access Exception: If immediate access is desired, the requesting party should contact the Director of Transportation Human Resources Division by telephone, who shall determine the outcome of the request.

D. **BROADCASTING E-MAIL MESSAGES**

If using a standard mailing list from the selection of lists provided by Information Services Division or any list of an employee's own creation that names most or all of the employees in an organization, one must have permission from the manager of the organization to which the list pertains.

For example, if an employee wishes to use the list named "Everybody in DOT," the employee must have permission from the office of the Secretary of Transportation. Likewise, selecting the "DOH" or "DMV" lists require permission from the office of the Commissioner of Highways or the Commissioner of Motor Vehicles, respectively.

Finally, whether or not an employee is using an official distribution list, the employee must ensure that all or most of the recipients have a reasonable need to see the message being sent.

E. **INQUIRIES AND POTENTIAL INFRACTIONS**

Because employees are charged with full compliance with this Policy, it is critical that they resolve any issues regarding interpretation or application by first consulting their organizational supervisors or their respective designees.

Each DOT employee is responsible for reporting any violation of these policies to his or her immediate supervisor. If the employee feels that his or her supervisor is not making an adequate effort to address the situation or is involved in it, he or she should report the issue(s) directly to the Director of Transportation Human Resources Division. This reporting should be done as discreetly as possible.

III. PENALTIES FOR VIOLATING POLICIES

Effective: 12/15/2007

Any violation of the preceding policies may result in disciplinary action, up to and including dismissal.

IV. APPENDICES

Effective: 12/15/2007

A. PROPER USE OF INFORMATION TECHNOLOGY POLICY ACKNOWLEDGEMENT STATEMENT

PROPER USE OF INFORMATION TECHNOLOGY POLICY ACKNOWLEDGEMENT STATEMENT

The Department's computers and other technological resources and equipment, as well as the network, DOT's email system and internet access, are for official use. Therefore, any information placed, created or transmitted in or through any of these resources belongs to the DOT, and that information, as well as any information accessed from these resources, may be monitored, searched, accessed, used, disclosed, and/or preserved by the DOT. The assignment or use of a User ID and/or password is not an indicator of privacy.

The use of any DOT computer or other technological equipment constitutes consent to these policies. There is no right of privacy in these systems and equipment, their content, or use.

This document certifies that I have **read** and **agree** to abide by the requirements set forth in the West Virginia Department of Transportation Volume I, Chapter 10 - Proper Use of Information Technology policy. As an employee of the West Virginia Department of Transportation, I **agree** to comply with these policies and acknowledge that I am personally liable for misuse or abuse of the agency's computers or other technological resources. I understand it is my responsibility to comply with these policies and specifically, avoid the prohibited uses and/or review my current use to make sure it complies with the current procedures.

NAME (print): _____

SIGNATURE: _____

LAST FOUR (4) DIGITS OF SOCIAL SECURITY NUMBER: ___ | ___ | ___ | ___

DATE: _____

ORGANIZATION NUMBER: _____

V. WVOT-PR1001 FORM
Effective: 12/01/08

Requesting a Technical Investigation of an Employee

Sections 1 through 3 must be filled out by Supervisors or Managers Only

Section 1

1. Supervisor or Manager Requesting Investigation _____

2. Title _____ 3. Agency _____ 4. Phone # _____

Section 2

1. Name of Individual to be Investigated _____

2. Email _____ 3. Userid _____

Section 3

1. Purpose of Investigation or Suspected Violation (see 4.1.3 of WVOT-PR1001, attach additional pages if necessary to explain) _____

2. Interval of Investigation From _____ To: _____

3. Report Due Date _____

Section 4

This section must ONLY be filled out by a Cabinet Secretary, a Commissioner, an Office Director, the Office of Special Investigations, or an Equivalent Authority:

1. Has the Technical Investigations procedure been read and understood? ___ Yes ___ No

2. Has the requestor provided sufficient information to initiate this investigation? ___Yes __ No

3. Does your Agency require Legal and/or Personnel approval for investigation actions? __Yes __No

4. If so, has this request been approved by your Agency Legal and/or Personnel Dept.? __Yes __No

5. (Print) Name_____ 6. Agency_____

7. Email _____ 8. Phone _____

9. Signature _____ 10. Date _____

This form must be forwarded to the Chief Information Security Officer (CISO) along with ALL supporting documentation. Send by Fax: (304) 558-1351 OR Mail: Office of Technology, One Davis Square, 321 Capitol Street, Charleston, WV 25301, Attn: CISO

Section 5 – ***Internal Use Only *

1.Has the investigator verified the authorizing signature? ____Yes ____No

2. Signature of Investigator _____ 3. Date _____